UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/920,801	08/03/2001	Taher Elgamal	06975-193002	8214

26171 7590 07/13/2005

FISH & RICHARDSON P.C.
P.O. BOX 1022
MINNEAPOLIS, MN 55440-1022

EXAMINER	
KLIMACH, PAULA W	
ART UNIT	**PAPER NUMBER**
2135	

DATE MAILED: 07/13/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/920,801	ELGAMAL ET AL.	
	Examiner	Art Unit	
	Paula W. Klimach	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *26 April 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *31-34,36-43 and 45-48* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *31-34, 36-43, and 45-48* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

This office action is in response to amendment filed on 04/26/2005. The amendment filed on 04/26/2005 have been entered and made of record. Therefore, presently pending claims are 31-34, 36-43, and 45-48.

Response to Arguments

Applicant's arguments filed 04/26/2005 have been fully considered the new grounds of rejection are found below.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 31, 38-39, 40, and 47-48 rejected under 35 U.S.C. 103(a) as being unpatentable over Klemba et al (5,651,068) in view of the Microsoft Press Computer Dictionary and further in view of Shrader et al (6,526,513).

In reference to claim 31 and 40, Klemba an apparatus and method for controlling cryptographic functions of an application program wherein the processor is configured to access a policy (column 6 line 20 in combination with column 7 lines 19-24) and that includes an attribute portion configured to store one or more cryptographic policy attributes and a value

portion having one or more attribute values, each attribute value corresponding to a cryptographic policy attribute and indicating whether an application program may use the cryptographic policy represented by the cryptographic policy attribute (column 6 lines 16-46). The information provided by the NFC during the initialization messages indicates attributes used by the policy. Further the processor selectively retrieves at least one of encryption information and decryption information from the policy file (column 6 line 58 to column7 line 18). The NFC retrieves the encryption algorithm for the CU to carry out the encryption (column 6 lines 27) and a back door for a third party to decrypt (column 7 lines 1-16). Further the processor selectively processes the retrieved encryption information and decryption information from the policy file in accordance with a predetermined capability condition and provides at least one of allowable encryption levels and decryption levels to the application program (column 5 lines 47-55).

Although Klemba discloses a cryptographic policy that collects data, Klemba does not expressly disclose that the policy is a file. The policy disclosed by Klemba permissions provided to the particular state, however Klemba does not expressly disclose the policy file containing the conditions of the policy file.

The Microsoft Press Computer Dictionary describes a file as named collection of information, such as a program, a set of data used by a program, or a user-created document. A file is the basic unit of storage that enables a computer to distinguish one set of information from another (page 194 definition of file).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to describe the policy in the NFC of Klemba as the claimed policy file. One of ordinary skill in the art would have been motivated to do this because a file is a collection of data

and the information stored on the NFC is a collection of data that is used by the CU. Klemba discloses a policy that involves the personalization of NFC (column 5 lines 64-67) therefore the personalized policy information is distinguished from other personalized policy information.

Shrader et al discloses a system wherein a policy file includes permissions that are granted and denied to the user (column 4 lines 1-24).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to maintain a file with permission that are denied and granted as in Shrader in a policy file in the system of Klemba. One of ordinary skill in the art would have been motivated to do this because it will enable the dynamic method of granting and denying permissions without rewriting security classes (Klemba column 1 lines 40-47).

In reference to claims 38 and 47, wherein each of the cryptographic policy attributes an indication of the cryptographic capabilities of the application program (column 5 lines 31-46), and each of the attribute values is one of a string, an integer number, and a truth expression (column 6 lines 16-45).

In reference to claims 39 and 48, wherein the truth expression is one of a true flag, a false flag, and a conditional flag (column 6 lines 16-46).

Claims 32-33 and 41-42 are rejected under 35 U.S.C. 103(a) as being unpatentable over Klemba et al (5,651,068) in view of the Microsoft Press Computer Dictionary and further in view of Shrader et al (6,526,513) as applied to claims 31 and 40 above, and further in view of Anderl et al (WO 87/07063).

Klemba, the Microsoft Dictionary, and Shrader do not expressly disclose the policy file comprising a JAVA archive file..

Anderl discloses the storage of multiple files on a smart card (page 2 lines 19-29). JAR files are Java class files. A smart card can contain multiple files as evidenced by Anderl; therefore can contain JAR files. The JAR files may contain digital signatures which are used for security as the files in Anderl that are credentials used for security.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to keep multiple files as in the file of Anderl in the system of Klemba. One of ordinary skill in the art would have been motivated to do this because the amount of files stored in a smart card is only limited by the amount of memory made available in the smart card. In addition the policy of Klemba can be divided into sub domain and files are a convenient method of organizing data.

In reference to claims 33 and 42, wherein the policy file comprises multiple component files, at least one of the component files storing some of the attribute portions and attribute values.

Although Klemba discloses the a states policies having sub domains (column 5 lines 31-55), Klemba does not discloses the policy being stored in multiple files

Anderl discloses the storage of multiple files on a smart card (page 2 lines 19-29).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to keep multiple files as in the file of Anderl in the system of Klemba. One of ordinary skill in the art would have been motivated to do this because the amount of files stored in a smart card is only limited by the amount of memory made available in the smart card. In

addition the policy of Klemba can be divided into sub domain and files are a convenient method of organizing data.

Claims 36-37 and 45-48 are rejected under 35 U.S.C. 103(a) as being unpatentable over Klemba et al (5,651,068) in view of the Microsoft Press Computer Dictionary and further in view of Shrader et al (6,526,513) as applied to claims 31 and 40 above, and further in view of and Schneier.

In reference to claims 36 and 45, although the combination of Klemba et al (5,651,068) in view of the Microsoft Press Computer Dictionary and further in view of Shrader et al (6,526,513) disclose the authentication of the NFC with the NCC and therefore a form of security, but do not disclose a form of security including a digital signature portion including at least one digital certificate for ensuring that the policy file has not been modified.

Schneier discloses the use of digital signatures to secure documents and make them unalterable (page 37 and 38)

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use digital signatures as in Schneier to secure the policies of Klemba. One of ordinary skill in the art would have been motivated to do this because it would ensure that the policy has not been altered and therefore encryption that is illegal in that nation-X is discouraged.

In reference to claims 37 and 46, wherein the signature portion applies to the policy file. The signature disclosed by Schneier refers to the part of the document that should not be altered in this case it would include the policy.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Paula W. Klimach whose telephone number is (571) 272-3854. The examiner can normally be reached on Mon to Thr 9:30 a.m to 5:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

PWK
Monday, July 11, 2005

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100